

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08248879 A**

(43) Date of publication of application: **27 . 09 . 96**

(51) Int. Cl.

G09C 1/00
G09C 1/00
H04L 9/06
H04L 9/32

(21) Application number: **08016512**

(22) Date of filing: **01 . 02 . 96**

(30) Priority: **06 . 02 . 95 US 95 384152**

(71) Applicant: **INTERNATL BUSINESS MACH
CORP <IBM>**

(72) Inventor: **ROGAWAY PHILLIP W
MIHIR BELLARE**

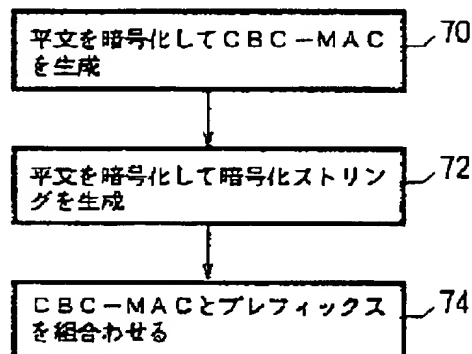
(54) **ENCRYPTION METHOD BY USING TWO KEY
AND DEVICE THEREFOR**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a deterministic and history-free plaintext string encryption method.

SOLUTION: An encryption method, by which a plaintext string is encrypted into a ciphertext, is started when the plaintext is encryption block chained (CBC) by using the first key and an empty initial setting vector and a CBC message check code (MAC) with a length equal to the block length is generated. Then, the plaintext string is encryption block chained again by using the second key and a CBC-MAC as an initial setting vector, and an encryption string is formed. Prefixes of the encryption string including all the blocks excepting the CBC-MAC and the final block are combined together, and the ciphertext is generated. In this process, an encryption using mode provided with a length maintenance property is also provided with a such a property as makes the related plaintext generate an unrelated ciphertext.

COPYRIGHT: (C)1996,JPO




Requested document: [JP8248879 click here to view the pdf document](#)

Method for data encryption/decryption using cipher block chaining (CBC) and message authentication codes (MAC)

Patent Number: [EP0725511](#), [A3](#)
Publication date: 1996-08-07
Inventor(s): ROGAWAY PHILLIP W (US); BELLARE MIHIR (US)
Applicant(s):: IBM (US)
Requested Patent: [JP8248879](#)
Application Number: EP19960300526 19960125
Priority Number(s): US19950384152 19950206
IPC Classification: H04L9/06
EC Classification: [H04L9/06](#)
Equivalents: [US5673319](#)

Abstract

A method for encrypting a plaintext string into ciphertext begins by cipher block chaining (CBC) (70) the plaintext using a first key and a null initialization vector to generate a CBC message authentication code (MAC) whose length is equal to the block length. The plaintext string is then cipher block chained (72) again, now using a second key and the CBC-MAC as the initialization vector, to generate an enciphered string. The CBC-MAC and a prefix of the enciphered string comprising all of the enciphered string except the last block are then combined (74) to create the ciphertext. The described mode of operation is length-preserving, yet has the property that related plaintexts give rise to unrelated ciphertexts. 

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-248879

(43) 公開日 平成8年(1996)9月27日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 1 0	7259-5 J	G 0 9 C 1/00	6 1 0 B
	6 4 0	7259-5 J		6 4 0 D
		7259-5 J		6 4 0 A
H 0 4 L 9/00		8842-5 J	H 0 4 L 9/00	6 1 1 A
9/32		8842-5 J		6 7 5 A
審査請求 未請求 請求項の数20 OL (全 12 頁)				

(21) 出願番号 特願平8-16512

(22) 出願日 平成8年(1996)2月1日

(31) 優先権主張番号 3 8 4 1 5 2

(32) 優先日 1995年2月6日

(33) 優先権主張国 米国 (US)

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)(72) 発明者 フィリップ・ダブリュー・ロガウェイ
アメリカ合衆国95616 カリフォルニア州
デービスアダムス・ストリート 850 ナンバー・エイ

(74) 代理人 弁理士 合田 潔 (外2名)

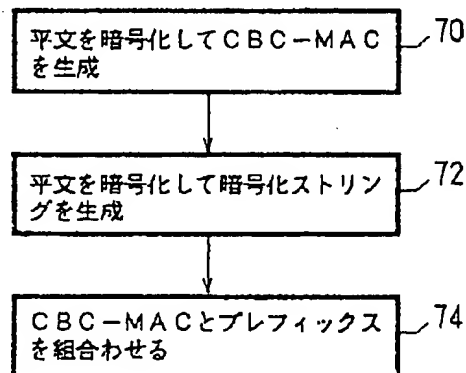
最終頁に続く

(54) 【発明の名称】 2つの鍵を使用して暗号化する方法および装置

(57) 【要約】

【課題】 決定論的かつヒストリ・フリーな平文ストリング暗号化方法を提供する。

【解決手段】 平文ストリングを暗号文に暗号化する方法が、第1の鍵および空初期設定ベクトルを使用して、平文を暗号ブロック連鎖 (CBC) し、ブロック長に等しい長さのCBCメッセージ確認コード (MAC) を生成することによって開始する。その後、平文ストリングは再び、今度は第2の鍵および初期設定ベクトルとしてのCBC-MACを使用して、暗号ブロック連鎖され、暗号化ストリングを生成する。CBC-MACおよび最終ブロックを除くすべてのブロックを含む暗号化ストリングのプレフィックスは、組み合わされて暗号文を生成する。ここでの暗号利用モードは、長さ保持性を備えながらも、関連する平文が、関連のない暗号文を生じさせるという特性を有している。



【特許請求の範囲】

【請求項1】第1および第2の鍵を使用して、平文ストリングを暗号文ストリングに暗号化する暗号化方法であって、

前記平文ストリングおよび前記第1の鍵を使用して、メッセージ確認コードを計算するステップと、

前記平文ストリング、前記第2の鍵、および前記メッセージ確認コードを使用して、実質的に前記メッセージ確認コードに依存する暗号化ストリングを生成するステップと、

前記暗号化ストリングの所定部分を前記メッセージ確認コードと組み合わせて前記暗号文ストリングを得るステップとを含む暗号化方法。

【請求項2】前記所定部分が前記暗号化ストリングの一部であることを特徴とする、請求項1に記載の暗号化方法。

【請求項3】前記メッセージ確認コードが、ブロック・サイファの暗号ブロック連鎖によって計算されることを特徴とする、請求項1に記載の暗号化方法。

【請求項4】前記ブロック・サイファが、DESである

【請求項5】前記所定部分が、前記暗号化ストリングから最終ブロックを除いたものであることを特徴とする、請求項2に記載の暗号化方法。

【請求項6】前記メッセージ確認コードが、ブロック長と等しい長さを有することを特徴とする、請求項2に記載の暗号化方法。

【請求項7】第1および第2の鍵を使用して、平文ストリングを暗号文ストリングに暗号化する方法であって、

(a) 前記第1の鍵および第1の初期設定ベクトルを使用して、前記平文ストリングを暗号ブロック連鎖し、長さがブロック長と等しいメッセージ確認コードを生成するステップと、

(b) 前記第2の鍵および第2の初期設定ベクトルとして前記メッセージ確認コードを使用して、前記平文ストリングを暗号ブロック連鎖し、暗号化ストリングを生成するステップと、

(c) 前記メッセージ確認コードおよび前記暗号化ストリングの所定部分を組み合わせて、前記暗号文ストリングを形成するステップとを含む方法。

【請求項8】前記所定部分が、前記暗号化ストリングから最終ブロックを除いたものであることを特徴とする、請求項7に記載の方法。

【請求項9】前記第1の初期設定ベクトルが、空ベクトルであることを特徴とする、請求項7に記載の方法。

【請求項10】前記平文ストリングの長さが、ブロック長の倍数に等しいことを特徴とする、請求項7に記載の方法。

【請求項11】前記平文ストリングの長さが、前記ブロック長の倍数に等しくないことを特徴とする、請求項7

に記載の方法。

【請求項12】ステップ(c)が、前記メッセージ確認コードおよび前記所定部分を連結して、前記暗号文ストリングを形成することを特徴とする、請求項7に記載の方法。

【請求項13】前記暗号文ストリングが、前記平文ストリングと等しい長さを有することを特徴とする、請求項7に記載の方法。

【請求項14】前記第1および第2の鍵が、秘密鍵から導き出されることを特徴とする、請求項7に記載の方法。

【請求項15】第1および第2の鍵ならびにブロック・サイファを使用して、メッセージ確認コードおよび暗号化ストリングを含む暗号文ストリングを平文ストリングに暗号解読する方法であって、

(a) 前記第2の鍵および初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記暗号化ストリングを暗号ブロック連鎖し、暗号解読ストリングを生成するステップと、

(b) 前記第1の鍵および空初期設定ベクトルを使用して、前記暗号解読ストリングを暗号ブロック連鎖し、最終ブロックを有するストリングを生成するステップと、

(c) 前記最終ブロックと、前記メッセージ確認コードにおける前記第1の鍵に基づくブロック・サイファの逆数との所定関数を計算するステップと、

(d) 前記暗号解読ストリングおよび前記所定関数の結果を組み合わせて、平文ストリングを生成するステップとを含む方法。

【請求項16】前記ブロック・サイファがDESであることを特徴とする、請求項15に記載の方法。

【請求項17】ステップ(c)における所定関数が、排他的論理和であることを特徴とする、請求項15に記載の方法。

【請求項18】記憶装置と、

平文ストリングを暗号文ストリングに暗号化するための、前記記憶装置においてサポートされたプログラム手段とを含み、

前記プログラム手段が、

前記平文ストリングおよび第1の鍵を使用してメッセージ確認コードを計算する手段と、

前記平文ストリング、第2の鍵、および前記メッセージ確認コードを使用して暗号化ストリングを生成する手段と、

前記暗号化ストリングの一部を前記メッセージ確認コードと組み合わせて前記暗号文ストリングを生成する手段とを含むことを特徴とするコンピュータ装置。

【請求項19】記憶装置と、

メッセージ確認コードおよび暗号化ストリングを含む暗号文ストリングを平文ストリングに暗号解読するための、前記記憶装置においてサポートされたプログラム手

段とを含み、
前記プログラム手段が、
秘密鍵および初期設定ベクトルとしての前記メッセージ
確認コードを使用して、前記暗号化ストリングを暗号ブ
ロック連鎖し、暗号解読ストリングを生成する手段と、
第2の秘密鍵および空初期設定ベクトルを使用して、前
記暗号解読ストリングを暗号ブロック連鎖し、最終ブロ
ックを有するストリングを生成する手段と、
前記最終ブロックと、前記第2の秘密鍵を使用して評価
されたブロック・サイファの逆数との所定関数を計算す
る手段と、
前記暗号解読ストリングおよび前記所定関数を組み合わ
せて前記平文ストリングを生成する手段とを含むことを
特徴とするコンピュータ装置。

【請求項20】第1および第2の鍵ならびにブロック・
サイファを使用して、暗号化および暗号解読を行うため
に、プロセッサによって実行される命令プログラムを記
憶し、該プロセッサによって読取り可能なプログラム記
憶装置であって、前記暗号化が、

(a) 前記第1の鍵および初期設定ベクトルを使用し
て、平文ストリングを暗号ブロック連鎖し、メッセージ
確認コードを生成するステップと、

(b) 前記第2の鍵および初期設定ベクトルとしての前
記メッセージ確認コードを使用して、前記平文ストリン
グを暗号ブロック連鎖し、暗号化ストリングを生成する
ステップと、

(c) 前記メッセージ確認コードおよび前記暗号化スト
リングの一部を組み合わせて暗号文ストリングを生成す
るステップとにより実行され、

前記暗号解読が、

(a) 前記第2の鍵および初期設定ベクトルとしての前
記メッセージ確認コードを使用して、前記暗号化ストリン
グを暗号ブロック連鎖し、暗号解読ストリングを生成
するステップと、

(b) 前記第1の鍵および空初期設定ベクトルを使用し
て、前記暗号解読ストリングを暗号ブロック連鎖し、最
終ブロックを有するストリングを生成するステップと、

(c) 前記最終ブロックと、前記メッセージ確認コード
における前記第1の鍵に基づくブロック・サイファの逆
数との所定関数を計算するステップと、

(d) 前記暗号解読ストリングおよび前記所定関数を組
み合わせて平文ストリングを生成するステップとにより
実行されることを特徴とする、プログラム記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般に安全な通信
に関し、より詳細には、平文を暗号文に暗号化するため
の方法に関する。

【0002】

【従来の技術】特定の特性を呈示する暗号化方式が、多

くの場合望ましいことは、一般に認められている。こう
した特性の第1は、多くの環境において使用可能もしくは
信頼に足る偶然性ソースは存在しないために、暗号化
および暗号解読操作が、確率的ではなく決定論的であ
るということである。また、方式がヒストリ・フリー
(過去の状態に関係しない)であるため、各暗号化または
暗号解読後に更新しなければならないメッセージ・カ
ウンタその他の情報を保存する必要がないということも
望ましい。この方式はまた、平文に関するあらゆる情報
を効果的に隠蔽するという点において、「安全」でなけ
ればならない。最後に、この方式が長さ保持性を備え
る、すなわち暗号文が平文の長さと同じことが望まし
い。

【0003】ブロック・サイファは、一般的な暗号化方
式を実施するために頻繁に使用される周知の暗号化ツ
ールである。ブロック・サイファは、(「1」ビットの)
固定長のメッセージ(平文)ブロックを、(「k」ピッ
トの)鍵の制御のもとに、等しい長さの暗号文ブロック
に変換する対称鍵暗号化システムである。広く使用され
るブロック・サイファは、米国標準DESアルゴリズム
によるものであり、 $l=64$ および $k=56$ を有し、1
977年1月米国商務省標準局発行「Data Encr
yption Standard」NBS FIPS
Pub 46に記載されている。DESのようなブロッ
ク・サイファは、文(たとえば、64ビット)の単一ブ
ロックを暗号化する方法をもたらす。しかし、それより
長いメッセージを暗号化するためには、ブロック・サイ
ファは、何らかの「暗号利用モード」において使用しな
ければならない。このような暗号利用モードの多くは、
従来技術において述べられてきたが、最も広く使用され
ているものは暗号ブロック連鎖(CBC)である。CB
Cについては、1980年12月米国商務省標準局発行
「DES Modes of Operation」N
BS FIPS Pub 81に記載されている。しか
し、CBCおよびその他の周知のモードは、長さが増加
してしまうか、もしくは明確な関連平文が関連暗号文を
生じさせるという欠点に煩わされるかのいずれかである。
前者を容認できない多くのアプリケーション・ドメ
インは、後者と効果的に妥協した独自のセキュリティを
備えている。

【0004】暗号ブロック連鎖(CBC)は、「初期設
定ベクトル」(IV)に加え、秘密鍵を必要とする。1
ービットのIV(その値は、メッセージと共に送られる
か、そうでない場合、両通信パーティに知られる)と
共に、ストリング $x=x_1 \dots x_n$ (それぞれが1ピッ
トの、 n ブロックから成る)は、 $E_{k,iv}(x)=y_1 \dots y_n$ と暗号化され、ここで $y_0=IV$ かつ $y_i=f_k(x_i+y_{i-1})$ である。CBC方式において、暗号
文の第1ブロックは、平文の最初のブロックに依存し、
暗号文の第2ブロックは、平文の最初の2つのブロック

5

に依存し、そしてさらに続き、暗号文の最終ブロックは、平文のすべてのブロックに依存する。しかし、このような暗号化は、IVが固定の場合、十分に安全とは言えないという点において周知の欠点を有している。

【0005】特に、CBC方式は、暗号化される平文についての情報を「漏洩」することもしばしばである。たとえば、敵対者がE_{1,iv}(X)とE_{1,iv}(X')を見て、最初の1ブロックが合致することに気づいたとすると、敵対者はXとX'もまた最初の1ブロックが合致すると推測することができる。このような欠点は非常に問題である。したがって、1Kバイトの従業員記録のシーケンスから成るファイルにおいて、7番目の記録以降が変更されていると気づかれたと仮定する。おそらくはまず、この変更が行われた理由は、誰かの降格により従業員記録を更新したためであると知られるであろう。暗号化方式が、E_{1,iv}であり、従業員記録が従業員名によるアルファベット順であれば、変更された従業員はアルファベット順で7番目にあった者であることが推測できる。

【0006】平文に関する情報を「漏洩」するCBC暗号化の上記の特徴には、初期設定ベクトルIVをランダムに選択し、そしてそれをメッセージと共に送ることによって対処できよう。しかし、これが行われると、方式は長さ保持性を失ってしまう。別法として、メッセージの暗号化は、ヒストリ依存(たとえば、IVをメッセージ・カウンタの関数として使用し、IVをメッセージと共に送らないことによって)で行うこともできるが、意図した受信者によるメッセージの不受信を容認しないために、この手法もまた満足とはいえない。

【0007】

【発明が解決しようとする課題】したがって、ブロック・サイファを使用する従来技術の暗号化技法は、長さの増加、メッセージの除去に対する非容認、または関連平文に関する情報の漏洩という点で望ましいものではない。従来技術におけるこれら他の問題を克服するブロック・サイファを使用する、安全で、長さ保持性を備える暗号化方式をもたらすことが依然として求められている。

【0008】したがって、本発明の主な目的は、決定論的かつヒストリ・フリーな平文ストリング暗号化の方法をもたらすことである。

【0009】本発明の他の目的は、暗号文の長さが、暗号化される平文の長さと同じ、暗号化のためのブロック・サイファ暗号利用モードをもたらすことである。

【0010】本発明の他の目的は、暗号化される平文に関する情報を漏洩することのない、長さ保持性を備える暗号化方式をもたらすことである。

【0011】本発明の他の目的は、各暗号化後または暗号解読後に更新しなければならないメッセージ・カウンタもしくは他の情報を、パーティが保存することがな

6

いように、ヒストリ・フリーなメッセージ暗号化方式をもたらすことである。

【0012】本発明の他の目的は、暗号ブロック連鎖(CBC)の新規な応用に基づく長さ保持性暗号化方式をもたらし、CBC暗号化に伴う周知の安全性および情報漏洩問題を克服することである。この技法は、暗号文メッセージをまだ見えない暗号文メッセージに改変すると、そのとき見える暗号文メッセージとは無関係の平文メッセージの暗号化が行われるので、極めて有利である。

【0013】本発明の他の目的は、1ブロックの長さの倍数または分数の長さを有する平文メッセージ・ストリングの暗号化を行う、新規な方法をもたらすことである。

【0014】

【課題を解決するための手段】本発明の以上のならびに他の目的は、第1および第2の秘密鍵を使用し、平文ストリングを暗号文ストリングに暗号化する方法において実施される。この方法は、最初に、第1の鍵および固定初期設定ベクトルを使用して平文ストリングの暗号ブロック連鎖を行うことにより、ブロックの長さと等しいCBCメッセージ確認コード(CBC-MAC)を生成する。その後、第2の鍵を使用し、また上記のCBCメッセージ確認コードを初期設定ベクトルとして使用する、平文ストリングの暗号ブロック連鎖が続き、これにより暗号化ストリングを生成する。CBCメッセージ確認コードおよび暗号化ストリングのプレフィックスは(通常は連結によって)組み合わされて、暗号文ストリングを形成する。この技法は、長さ保持性を備える、すなわちプレフィックスが最終ブロックを除くすべてのブロックを含むため、暗号文の長さが平文の長さと同じになっていることが、望ましい。

【0015】したがって、好ましい方法にしたがい、平文ストリングは、CBCを2度使用して処理されるが、まずCBC-MACを生成し、次に暗号文自体の一部を生成する。第1のパスにおいては、CBCで使用する初期設定ベクトルは、空ベクトル(ブロック長さに等しい長さを有する0ビットのストリングを意味する)である。第2のパスにおいては、初期設定ベクトルは、第1パスで生成されたCBC-MACである。この2つのパスに対する鍵は、別個である。この方法は、平文ストリングが、1つのブロックの長さの倍数の長さを有する場合、暗号文を生成するのに有用である。この方式の変形例は、平文ストリングが、このブロックの長さの分数である場合に使用することができる。

【0016】暗号文を暗号解読するためには、第2の鍵およびCBC-MACを初期設定ベクトルとして使用して、暗号化ストリング部分が暗号ブロック連鎖され、暗号解読ストリングを生成する。そして暗号解読ストリングは、第1の鍵と空IVを使用して、暗号ブロック連鎖

され、最後のブロックを有するストリングを生成する。その後平文は、暗号解読ストリングと最終ブロックの所定関数（たとえば、排他的論理和XOR）、およびCBC-MACにおける第1の鍵に基づくブロック・サイファの逆数の組合せとして得られる。

【0017】本発明の他の目的は、このような方法を、プログラムされたコンピュータにおいてまたは専用ハードウェアやソフトウェアで実施することである。1つの実施例においては、本発明の様々な方法は、プロセッサによって読取り可能であり、各方法の様々な処理ステップを行うためにプロセッサによって実行される命令プログラムを具体的に実施する、プログラム記憶装置（たとえば、フロッピー・ディスク）上で実施することができる。

【0018】以上は、本発明のより関連のある目的の概略を述べたものである。これらの目的は、本発明のより顕著な特徴および用途を単に例示したものと解釈されたい。ここに開示する発明を、異なる方法で適用することによって、もしくは以下に述べるように本発明に変更を加えることによって、多くの他の有利な結果を得ることができる。したがって、以下の好ましい実施例についての詳細な記述を参照することにより、本発明の他の目的およびさらに深い理解が得られるであろう。

【0019】

【発明の実施の形態】簡単な背景として、本発明のサポートに使用するコンピュータが図1に示されている。コンピュータ20は、システム・ユニット21、キーボード22、マウス23および表示装置24を含んでいる。表示装置24の画面26は、グラフィカル・ユーザ・インターフェース（GUI）を呈示するために使用される。オペレーティング・システムによってサポートされたグラフィカル・ユーザ・インターフェースにより、ユーザは、指示して選ぶ入力方法を使用する、すなわちマウス・ポインタ25を、画面26上の特定位置のデータ・オブジェクトを表すアイコンまで移動させ、マウス・ボタンを押してユーザ命令または選択を実行することができる。

【0020】図2は、図1に示されたパーソナル・コンピュータの構成要素を示すブロックダイアグラムである。システム・ユニット21は、様々な構成要素が接続され、様々な構成要素間の通信が行われる、1つまたは複数のシステム・バス31を含んでいる。マイクロプロセッサ32は、システム・バス31に接続されており、同様にシステム・バス31に接続された読取り専用メモリ（ROM）33およびランダムアクセス・メモリ（RAM）34によってサポートされている。IBM PS/2シリーズ・コンピュータに搭載されているマイクロプロセッサは、386や486マイクロプロセッサなどのIntel系マイクロプロセッサの1つである。68000、68020、68030マイクロプロセッサのよ

うな、Motorola系マイクロプロセッサ、IBM社製PowerPC[®]マイクロプロセッサのような様々なRISCマイクロプロセッサ、およびHewlett Packard、Sun、Intel、Motorola他により製造された他のマイクロプロセッサも、特定のコンピュータにおいて使用することができるが、これらに限定するものではない。

【0021】ROM33は、他のコードと共に、対話のような基本的ハードウェア動作およびディスク・ドライブやキーボードを制御する基本入出力システム（BIOS）を含んでいる。RAM34は、オペレーティング・システムおよびアプリケーション・プログラムがロードされるメイン・メモリである。メモリ管理チップ35は、システム・バス31に接続され、RAM34、ハード・ディスク・ドライブ36、フロッピー・ディスク・ドライブ37の間でデータをやりとりするなどの、ダイレクト・メモリ・アクセス動作を制御する。同様にシステム・バス31に接続されたCD ROM42は、たとえばマルチメディア・プログラムや大規模データベースなどの大容量データを保存するために使用される。

【0022】その他にこのシステム・バス31に接続されているのは、キーボード・コントローラ38、マウス・コントローラ39、ビデオ・コントローラ40、オーディオ・コントローラ41などの、様々な入出力コントローラである。キーボード・コントローラ38は、キーボード22のハードウェア・インターフェースをもたらし、マウス・コントローラ39は、マウス23のハードウェア・インターフェースをもたらし、ビデオ・コントローラ40は、表示装置24にハードウェア・インターフェースをもたらし、オーディオ・コントローラ41は、スピーカー25aと25bにハードウェア・インターフェースをもたらし、トークン・リング・アダプタのような入出力コントローラ50は、ローカル・エリア・ネットワーク56を介して他の同様に構成されたデータ処理システムへの通信を可能にしている。

【0023】本発明の好ましい実施例の1つは、ランダム・アクセス・メモリ34内に常駐するコード・モジュール内の命令セットとしてのものである。コンピュータ・システムによって要求されるまで、命令セットは他のコンピュータ・メモリ、たとえばハード・ディスク・ドライブ36内、またはCD ROM42で最終的に使用される光ディスクもしくはフロッピー・ディスク・ドライブ37で最終的に使用されるフロッピー・ディスクのような取外し可能メモリ内に保存されている。さらに、ソフトウェアによって選択的に活動化または再構成される汎用コンピュータにおいて、本明細書に記載の様々な方法が好都合に実施されるが、このような方法は、必要な方法ステップを実行するように構成されたハードウェア、ファームウェア、またはさらに特殊な装置においても実行できる。

【0024】本発明の方法は、図1に示されたようなコンピュータ上で実施されることを意図したものであるが、「コンピュータ」という用語には、最も広い範囲と意味が与えられ、特定のアプリケーションには関わりなく計算機能をもたらす任意のタイプの装置またはその一部を含むことに留意されたい。

【0025】ここで図3を参照すると、平文ストリングを暗号文に暗号化する好ましい方法が、流れ図により示されている。暗号化パーティおよび暗号解読パーティが、1対の秘密鍵（すなわち第1および第2の鍵）を共用するものと仮定する。ステップ70において、平文ストリングは、第1の（秘密）鍵および空初期設定ベクトル（IV）を使用して暗号ブロック連鎖され、暗号文の最終ブロックであるCBCメッセージ確認コード（MAC）を生成する。ステップ72において、平文ストリングは、今度は第2の（秘密）鍵および初期設定ベクトルとしてのCBC-MAC（ステップ70で生成）を使用して、再び暗号ブロック連鎖され、これにより暗号化ストリングを生成する。ステップ74において、CBC-MAC（ステップ70で生成）および暗号化ストリング（ステップ72で生成）の一部が組み合わされて暗号文を生成する。この暗号化ストリングの部分は、「プレフィックス」とも呼ばれる。この組合せはさらに第1の鍵の関数である。

【0026】暗号文（図3のルーチンにより生成）の暗号解読は、図4において示されている。ステップ76において、暗号化ストリング（ステップ72で生成）は、第2の秘密鍵および初期設定ベクトルとしてのCBC-MAC（ステップ70で生成）を使用して、暗号ブロック連鎖によって暗号解読される。ステップ76は、暗号解読ストリングを生成する。ステップ78において、暗号解読ストリングは、第1の鍵および空IVを使用して、暗号ブロック連鎖され、最終ブロックを有するもう1つのストリングを生成する。ステップ80において、この最終ブロックと第1の鍵に基づくCBC-MAC（ステップ70で生成）におけるブロック・サイファの逆数との所定関数が計算される。続いて平文が、ステップ82において、暗号解読ストリングおよび所定関数の結果の組合せ（すなわち連結）として形成される。

【0027】暗号化ルーチンのステップ70および72における動作は、それぞれ図5および6に示されている。このルーチンは、鍵の長さ k を有する1ビット・ブロック・サイファ f （DESのような）を使用する。 k ビット鍵 a を使用して1ビットの x に適用されたブロック・サイファの値である1ビットのストリングを $f_a(x)$ で表す。さらに、上記のように、第1の鍵 a_0 および第2の鍵 a_1 がルーチンに使用可能であり、 $|a_0| = |a_1| = k$ であると、初めに仮定する。これらの鍵は、標準鍵分離技法を使用して、見えない k ビットの鍵 K から導き出すことができる。たとえば、 a_0 は f

$f_a(0)$ の最初の k ビットであり、 a_1 は $f_a(1)$ の最初の k ビットとなる。図5において、平文ストリングは、メッセージ・ストリング x から構成されており、これは例示のためにそれぞれ64ビットのブロックが10、すなわち合計640ビットを含むものと仮定する。したがって、メッセージ・ストリングは、 $x = x_1 x_2 \dots x_{10}$ である。このストリングは、暗号ブロック連鎖暗号化ルーチン82に供給され、これはまた第1の鍵 a_0 および空初期設定ベクトル（すなわち $IV = 0$ ）を受け取る。暗号ブロック連鎖ルーチン82の結果は、出力ストリング $y = y_1 y_2 \dots y_{10}$ である。最終ブロック y_{10} は、64ビットの暗号ブロック連鎖メッセージ確認コード、すなわち「CBC-MAC」である。これでルーチンの第1パスは終了する。

【0028】第2パスは、図6において示され、ここでメッセージ・ストリング（すなわち平文）は、再び暗号ブロック連鎖暗号化ルーチン82に供給される。しかし、このパスにおいては、ルーチンによって使用される鍵は、第2の（秘密）鍵 a_1 であり、初期設定ベクトルは、図5に示された第1のパスにおいて生成されたCBC-MAC（すなわち y_{10} ）である。結果として生成した暗号化ストリングは、 $y' = y'_1 y'_2 \dots y'_{10}$ である。このプロセスで第2のパスが終了する。図5および図6において示されたブロック・サイファ f は同一であるが、これは必須ではないことに留意されたい。そして暗号文は、CBC-MACおよび暗号化ストリングの一部を組合せて（たとえば、連結によって）得られる。すなわち、

暗号文 $= y_{10} \parallel y'_1 y'_2 \dots y'_9$

暗号文の長さが平文ストリングの長さと同じで、このルーチンは、長さ保持性を備える。「 \parallel 」は連結を表す。

【0029】10ブロックのストリング y を暗号解読するために、まずこれを一連のブロックと考える。

$y_{10} \parallel y'_1 y'_2 \dots y'_9$

暗号解読ルーチンの各ステップ76、78、80における動作は、それぞれ図7、図8、図9において示された通りである。図7に示されるように、ステップ76は、第2の鍵 a_1 およびIVとしてのCBC-MAC（すなわち、 y_{10} ）を使用して暗号化ストリング $y'_1 y'_2 \dots y'_9$ （ステップ72で生成）のCBC暗号解読84を含んでいる。結果として暗号解読されたストリングは、 $x_1 x_2 \dots x_9$ であり、これは元の平文のほとんどすべてを表している。 x_{10} を復元するために、暗号解読ルーチンはまず、図8に示す操作を行い、ここで解読されたストリング $x_1 x_2 \dots x_9$ は、第1の鍵 a_0 と空IVを使用して暗号化され（CBC84により）、最終ブロックが y_9 であるストリング $y_1 y_2 \dots y_9$ を生成する。図9から見て取れるように、 y_9 と、 y_{10} における第1の鍵に基づくブロック・

サイファ f の逆関数と、所定関数 86 (たとえば、XOR) が計算されて x_{10} を生成する。その後、平文は、以下ようになる。

平文 = $x_1 x_2 \dots x_9 \parallel x_{10}$

【0030】上記の好ましい実施例では、ステップ72 および76におけるブロック・サイファの暗号利用モードとして暗号ブロック連鎖を使用している。しかし、他の暗号利用モードもこうしたステップに使用することができるため、本発明は、さほど限定されたものではない。さらに、暗号ブロック連鎖が、メッセージ確認コードを生成するために平文に対する第1のパス(ステップ70)において好ましく使用されているが、他の周知のMAC(もしくは他のブロック・サイファ連鎖モード)生成の技法を、このステップにおいてCBCに代えて代用することができることに留意されたい。(唯一必要なことは、 m の1ビットのMACおよび m の特定1ビット以外のすべてのビットが与えられると、脱落している1ビットは、効果的かつ一意的に再構成可能である。)したがって、本発明によれば、平文ストリングを処理する第1のパスは、メッセージ確認コードまたはタグを計算する第1の鍵 a_0 を使用する周知の技法を含むものと想定される。上記のように、第2のパスは、このMACをIVとして第2の鍵 a_1 と共に使用してメッセージを暗号化ストリングに暗号化することを含んでいる。この第2のパスは、CBCを使用して行うことができるが、これは必須ではない。MACおよび暗号化ストリングの一部は、暗号文として得られる。

【0031】したがって、本発明のより一般的な態様によれば、暗号化は、メッセージ確認コードを計算するために、平文ストリングおよび第1の鍵の使用を伴う。このルーチンは、メッセージ、第2の鍵、およびメッセージ確認コードを使用することによって継続して、メッセージ確認コードに実質的に依存する暗号化ストリングを*

$$F_{a0}^{(s)}(m) = f_{a0}(f_{a0}(\dots(f_{a0}(m_1) \oplus m_2) \oplus \dots \oplus m_{s-1}) \oplus m_s)$$

【0033】ここで x が、暗号化しようとするメッセージであり、 $1 \leq |x| < 2^l$ と仮定する。 $x = x_1 \dots x_{n-1} x_n$ を、暗号化されるメッセージとし、ここで $|x_1| = \dots = |x_{n-1}| = 1$ かつ $|x_n| \leq 1$ とする。仮定 $|x_1| \geq 1$ は、暗号化すべき「フル」ブロックが少なくとも1つあることを意味することに留意されたい。次の方法は、1未満の長さのメッセージには適用すべきではない。

【数2】

$$x' = \langle |x| \rangle x_1 \dots x_{n-3} x_{n-2} x_n 0^{1-|x_n|} x_{n-1}$$

とする。上記のステップではまず、メッセージ・ストリングを後続ゼロで埋め、暗号化されるストリングの全長が、確実にブロック長の倍数になるようにし、それから x の(以前は短かった)最終ブロックを、 x の第2から

*生成する。このような「実質的」依存とは、暗号化ストリングのすべてのビットが、MACが異なる値をとるにつれて変化することを意味している。平文の暗号文は、メッセージ確認コードおよび暗号化ストリングの一部と共に含む形態で得られる。このプロセスを逆行させるために、暗号解読ルーチンには、暗号文の暗号化ストリング部分、第2の鍵およびMACを使用して暗号解読ストリングを生成することが含まれる。暗号解読は、暗号解読ストリングおよび第1の鍵を使用して最終ブロックを有するストリングを生成することによって継続する。そして、最終ブロックおよびMACにおける第1の鍵に基づくブロック・サイファの逆数の既定関数が計算される。平文は、暗号解読ストリングおよび既定関数の結果として得られる。

【0032】本発明のより詳細な実施例を、以下に述べる。この実施例では、処理される特定のストリングが、所望のブロック長と等しいかまたはその分数であろうとなかろうと、メッセージ・ストリングを処理する。この方法は、長さ k の鍵と共に1ビットのブロック・サイファ f を選択することにより開始する。たとえば、 f がDESアルゴリズムである場合、 l は64である。もちろん、DESに加えて他のブロック・サイファ(たとえば、IDEAまたはSKIPJACK)も使用することができる。秘密鍵を、 $a = (a_0, a_1)$ 、ここで $|a_0| = |a_1| = k$ とし、また λ が空ストリング($0^k = \lambda$)を表すものとする。秘密鍵 a_0 および a_1 は、(少なくとも実際の計算に関しては)相互関係はないものとする。 $\langle m \rangle$ が、数 $m < 2^l$ を1ビットのブロックに符号化することを表すものとする。それぞれ1ビットの、 s ブロックから成るストリング $m = m_1 \dots m_s$ に対し、 a_0 における m の(1ビット)CBC-MACは、次のように定義される。

【数1】

最終に至る(フル)ブロックと入れ換える。(メッセージの長さが、ブロック長の倍数である場合は、このステップは必須ではない)ここで、 $x' = x_1 \dots x_{n-2} x_n$ とする。 $|x'| = |x| = 1$ であることに留意されたい。

【0034】暗号化方式E、(・)は次の通りである。

・ステップ1.

【数3】

$$t = f_{a0}^{(n+1)}(x')$$

を、 a_0 における x' の1ビットのCBC-MACとする。

・ステップ2. x' を次のように暗号化する。 $y_0 = t$ (すなわち初期設定ベクトル)とする。そして、 $i = 1, \dots, n-2$ に対し、

13

【数4】

$$y_i = f_{a1}(x_i \oplus y_{i-1})$$

とする。最後に、 $|x_n| = 1$ の場合、

【数5】

$$y_n = f_{a1}(x_n \oplus y_{n-2})$$

とする。そうでない場合（すなわち $1 \leq |x_n| < 1$ ）、 y_n を、 $f_{a1}(y_{n-2})$ の最初の $|x_n|$ ビットと x_n とのXORとする。この暗号化方法は、可変長ブロックにも適用可能なCBC暗号利用モードの拡張機能である。（ブロック・サイファがDESである場合、この方法は、IBM CUSP/3848メカニズムと呼ばれている。）

・ ステップ3. $E_i(x) = t y_1 \dots y_{n-2} y_n$ と定義する。すなわち、 x の暗号化は、ステップ2からの暗号文を伴う t である。

【0035】受信した暗号文を $y = t y_1 \dots y_{n-2} y_n$ として、暗号解読は、次のように行われる。

・ ステップ1. 鍵 a_1 で暗号文 $y_1 \dots y_{n-1} y_n$ を暗号解読することによって、 x^* を復元する。すなわち、 $y_0 = t$ とし、 $i = 1, \dots, n-2$ に対し、

【数6】

$$x_i = f_{a1}^{-1}(y_i) \oplus y_{i-1}$$

とする。

【数7】

$$|y_n| = 1$$

の場合

【数8】

$$x_n = f_{a1}^{-1}(y_n) \oplus y_{n-2}$$

とする。そうでない場合（すなわち $1 \leq |y_n| < 1$ ）、 x_n を、 $f_{a1}(y_{n-2})$ の最初の $|y_n|$ ビットと y_n とのXORとする。

・ ステップ2. x_{n-1} を復元するために、

【数9】

$$t' = f_{a0}^{(n)}(|y| x_1 \dots x_{n-2} x_n 0^{1-|x_n|})$$

とし、

【数10】

$$x_{n-1} = f_{a0}^{-1}(t') \oplus t'$$

とする。復元された平文は、 $x_1 \dots x_n$ である。

【0036】本発明は、暗号化が長さ保持性を備え、過去の状態に関係せず、決定論的かつ安全であるという点において、重要な利点をもたらす。関連する暗号化方法は、こうした初期的要求事項を達成できるだけでなく、さらに、ハードウェア、ソフトウェアいずれにおいて

14

も、完全に並列使用を確かなものにする。たとえば、メッセージ確認コード t は米国特許第4,933,969号に記載の「ツリーMAC」方式により計算することができる。暗号化機能には、単に、メッセージ x と $f_{a1}(t) f_{a1}((t+1) \bmod 2^1) f_{a1}((t+2) \bmod 2^1) \dots$ の長さ $|x|$ のプレフィックスとのXORをとることが含まれる。このような実施例に基づき、プロセッサの効率を2倍にすることは、暗号文が計算される速度を2倍にすることになる。

【0037】本明細書に記載の方法の具体的な適用例は、多岐にわたる。たとえば、この技法は、プロトコル・データ・ユニットのフィールドの暗号化、ファイルの「1ノード」に依存しない方法でのファイルの暗号化、または物理媒体におけるセクタ位置に依存しないディスク・セクタの暗号化に有用である。最初の例は、いくつかのメッセージ・ビットが不用意に使用可能になるような通信プロトコルがある場合に行われ得る。各フィールドのビット数を変えずに、安全性を高めることが望ましい。言い替えれば、かつて明文で転送されたメッセージのすべてを暗号化して送ることができることが望ましい。

【0038】以上開示された特定の実施例は、本発明と同様の目的を達成するための他のルーチンを変更または設計する基礎として容易に利用することができる。このような均等技法および実施例は、本発明の精神および範囲を逸脱するものではない。

【0039】まとめとして、本発明の構成に関して以下の事項を開示する。

【0040】(1) 第1および第2の鍵を使用して、平文ストリングを暗号文ストリングに暗号化する暗号化方法であって、前記平文ストリングおよび前記第1の鍵を使用して、メッセージ確認コードを計算するステップと、前記平文ストリング、前記第2の鍵、および前記メッセージ確認コードを使用して、実質的に前記メッセージ確認コードに依存する暗号化ストリングを生成するステップと、前記暗号化ストリングの所定部分を前記メッセージ確認コードと組み合わせて前記暗号文ストリングを得るステップとを含む暗号化方法。

(2) 前記所定部分が前記暗号化ストリングの一部であることを特徴とする、上記(1)に記載の暗号化方法。

(3) 前記メッセージ確認コードが、ブロック・サイファの暗号ブロック連鎖によって計算されることを特徴とする、上記(1)に記載の暗号化方法。

(4) 前記ブロック・サイファが、DESであることを特徴とする、上記(2)に記載の暗号化方法。

(5) 前記所定部分が、前記暗号化ストリングから最終ブロックを除いたものであることを特徴とする、上記(2)に記載の暗号化方法。

(6) 前記メッセージ確認コードが、ブロック長と等しい長さを有することを特徴とする、上記(2)に記載の

暗号化方法。

(7) 第1および第2の鍵を使用して、平文ストリングを暗号文ストリングに暗号化する方法であって、(a) 前記第1の鍵および第1の初期設定ベクトルを使用して、前記平文ストリングを暗号ブロック連鎖し、長さがブロック長と等しいメッセージ確認コードを生成するステップと、(b) 前記第2の鍵および第2の初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記平文ストリングを暗号ブロック連鎖し、暗号化ストリングを生成するステップと、(c) 前記メッセージ確認コードおよび前記暗号化ストリングの所定部分を組み合わせ、前記暗号文ストリングを形成するステップとを含む方法。

(8) 前記所定部分が、前記暗号化ストリングから最終ブロックを除いたものであることを特徴とする、上記(7)に記載の方法。

(9) 前記第1の初期設定ベクトルが、空ベクトルであることを特徴とする、上記(7)に記載の方法。

(10) 前記平文ストリングの長さが、ブロック長の倍数に等しいことを特徴とする、上記(7)に記載の方法。

(11) 前記平文ストリングの長さが、前記ブロック長の倍数に等しくないことを特徴とする、上記(7)に記載の方法。

(12) ステップ(c)が、前記メッセージ確認コードおよび前記所定部分を連結して、前記暗号文ストリングを形成することを特徴とする、上記(7)に記載の方法。

(13) 前記暗号文ストリングが、前記平文ストリングと等しい長さを有することを特徴とする、上記(7)に記載の方法。

(14) 前記第1および第2の鍵が、秘密鍵から導き出されることを特徴とする、上記(7)に記載の方法。

(15) 第1および第2の鍵ならびにブロック・サイファを使用して、メッセージ確認コードおよび暗号化ストリングを含む暗号文ストリングを平文ストリングに暗号解読する方法であって、(a) 前記第2の鍵および初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記暗号化ストリングを暗号ブロック連鎖し、暗号解読ストリングを生成するステップと、(b) 前記第1の鍵および空初期設定ベクトルを使用して、前記暗号解読ストリングを暗号ブロック連鎖し、最終ブロックを有するストリングを生成するステップと、(c) 前記最終ブロックと、前記メッセージ確認コードにおける前記第1の鍵に基づくブロック・サイファの逆数との所定関数を計算するステップと、(d) 前記暗号解読ストリングおよび前記所定関数の結果を組み合わせ、平文ストリングを生成するステップとを含む方法。

(16) 前記ブロック・サイファがDESであることを特徴とする、上記(15)に記載の方法。

(17) ステップ(c)における所定関数が、排他的論理和であることを特徴とする、上記(15)に記載の方法。

(18) 記憶装置と、平文ストリングを暗号文ストリングに暗号化するための、前記記憶装置においてサポートされたプログラム手段とを含み、前記プログラム手段が、前記平文ストリングおよび第1の鍵を使用してメッセージ確認コードを計算する手段と、前記平文ストリング、第2の鍵、および前記メッセージ確認コードを使用して暗号化ストリングを生成する手段と、前記暗号化ストリングの一部を前記メッセージ確認コードと組み合わせ、前記暗号文ストリングを生成する手段とを含むことを特徴とするコンピュータ装置。

(19) 記憶装置と、メッセージ確認コードおよび暗号化ストリングを含む暗号文ストリングを平文ストリングに暗号解読するための、前記記憶装置においてサポートされたプログラム手段とを含み、前記プログラム手段が、秘密鍵および初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記暗号化ストリングを暗号ブロック連鎖し、暗号解読ストリングを生成する手段と、第2の秘密鍵および空初期設定ベクトルを使用して、前記暗号解読ストリングを暗号ブロック連鎖し、最終ブロックを有するストリングを生成する手段と、前記最終ブロックと、前記第2の秘密鍵を使用して評価されたブロック・サイファの逆数との所定関数を計算する手段と、前記暗号解読ストリングおよび前記所定関数を組み合わせ、前記平文ストリングを生成する手段とを含むことを特徴とするコンピュータ装置。

(20) 第1および第2の鍵ならびにブロック・サイファを使用して、暗号化および暗号解読を行うために、プロセッサによって実行される命令プログラムを記憶し、該プロセッサによって読取り可能なプログラム記憶装置であって、前記暗号化が、(a) 前記第1の鍵および初期設定ベクトルを使用して、平文ストリングを暗号ブロック連鎖し、メッセージ確認コードを生成するステップと、(b) 前記第2の鍵および初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記平文ストリングを暗号ブロック連鎖し、暗号化ストリングを生成するステップと、(c) 前記メッセージ確認コードおよび前記暗号化ストリングの一部を組み合わせ、暗号文ストリングを生成するステップとにより実行され、前記暗号解読が、(a) 前記第2の鍵および初期設定ベクトルとしての前記メッセージ確認コードを使用して、前記暗号化ストリングを暗号ブロック連鎖し、暗号解読ストリングを生成するステップと、(b) 前記第1の鍵および空初期設定ベクトルを使用して、前記暗号解読ストリングを暗号ブロック連鎖し、最終ブロックを有するストリングを生成するステップと、(c) 前記最終ブロックと、前記メッセージ確認コードにおける前記第1の鍵に基づくブロック・サイファの逆数との所定関数を計算す

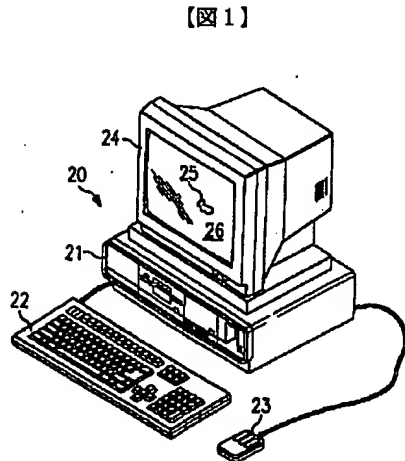
るステップと、(d) 前記暗号解読ストリングおよび前記所定関数を組み合わせて平文ストリングを生成するステップとにより実行されることを特徴とする、プログラム記憶装置。

【図面の簡単な説明】

【図 1】 本発明の暗号化および暗号解読方式の実施に使用する、システム・ユニット、キーボード、マウスおよび表示装置を含むコンピュータを示す図である。

【図 2】 図 1 に示されたコンピュータの構造を示すブロック図である。

【図 3】 平文を暗号文に暗号化する本発明の方法を示す簡略化流れ図である。



【図 4】 暗号文 (図 3 において生成された) が、どのように変換されて平文に戻されるかを示す、簡略化流れ図である。

【図 5】 図 3 のステップ 70 を示す図である。

【図 6】 図 3 のステップ 72 を示す図である。

【図 7】 図 4 のステップ 76 を示す図である。

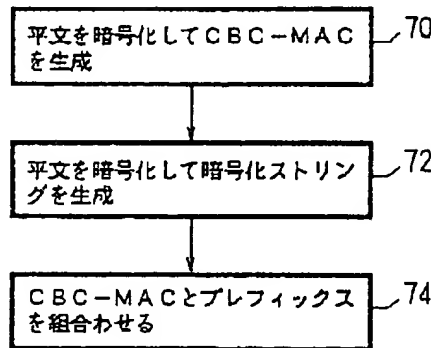
【図 8】 図 4 のステップ 78 を示す図である。

【図 9】 図 4 のステップ 80 を示す図である。

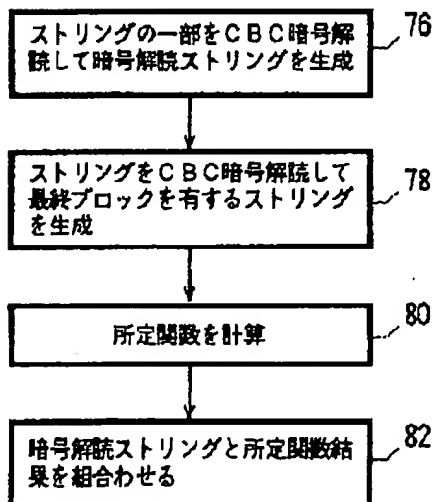
【符号の説明】

- 10 70 平文を暗号化して CBC-MAC を生成
72 平文を暗号化して暗号化ストリングを生成
74 CBC-MAC とプレフィックスを組み合わせる

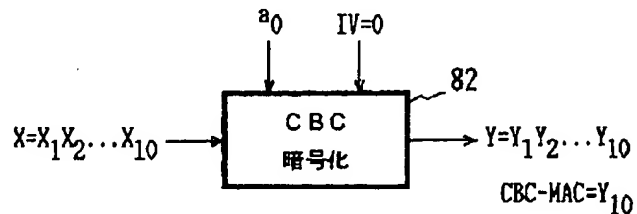
【図 3】



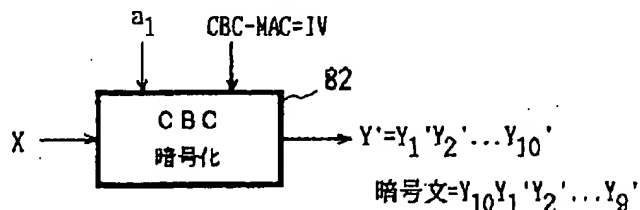
【図 4】



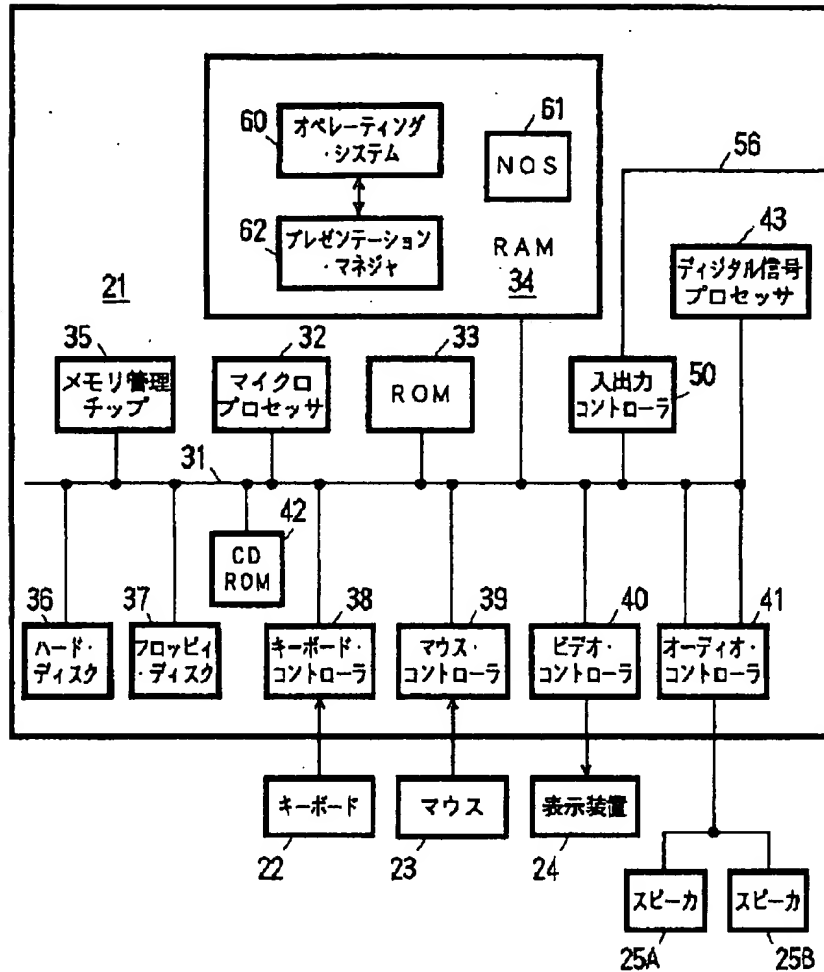
【図 5】



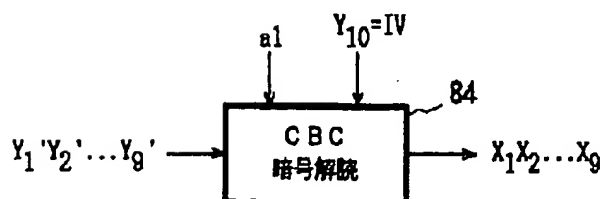
【図 6】



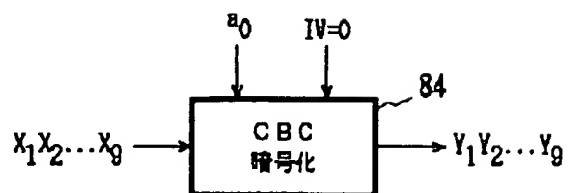
【図2】



【図7】



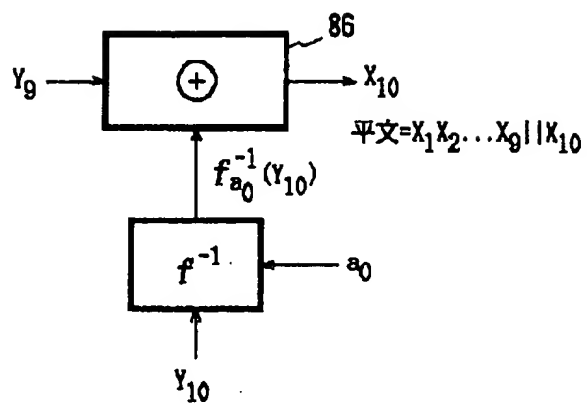
【図8】



(12)

特開平 8 - 2 4 8 8 7 9

【図 9】



フロントページの続き

(72)発明者 ミヒル・ペラール
 アメリカ合衆国10532 ニューヨーク州ホ
 ーソンセントラル・パーク・ウェスト
 372